Cisco Unified Communications 14SU2
COP File for CDETS CSCwc26596

Release Notes Version 3
Jun 14, 2023

Introduction:

This readme contains important information about the installation procedures for the COP file for the 14SU2 release of Cisco Unified Communications products. This COP file, ***ciscocm.V14-SU2-SU2a_CSCwc26596_C0169-1.k4.cop.sha512*** is only designed for the following products and versions:

CUCM: 14.0.1.12900-161 and 14.0.1.13024-2
CUC: 14.0.1.12900-69
IM&P: 14.0.1.12900-6 and 14.0.1.12901-1

Note: Before you install this update, Cisco recommends that you review the *Important Notes* section for information about issues that may affect your system.

What this COP file provides:

This COP file provides a fix to address the following issue:

CSCwc26596: Unable to upload Signed CA certs if Signer certs has initial identical words

Related Documentation:

To view documentation that supports your version of Cisco Unified Communications Manager release, go to: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.html

Determining the Software Versions:

Cisco Unified Communications Manager

You can determine the System Version of the Cisco Collaboration Product software that is running on your server by accessing Cisco Unified Operating System Administration Web page.

The following information displays:

- System version: xxxxx

Important Notes:

This COP file should be installed on all nodes in the cluster.

The Cisco Tomcat service will be restarted as part of the COP file install. As such, the COP file should be installed via the CLI, not the GUI. It should also be installed individually on all nodes, not using the "utils upgrade cluster" command.

A reboot is not required as part of the COP file install.

NOTE: After installing this COP file, it's been seen where RTMT can no longer connect to all nodes in the cluster for trace collection, only the node RTMT was pointed to will display as available to collect logs from. This is due to internal Trace Collection Service port bindings between nodes that need to be refreshed.

The workaround for this is to manually restart the following 2 services on all nodes:

Cisco Trace Collection Service
Cisco Trace Collection Servlet

Note for CUC Installs:
For Cisco Unity Connection, the following services need to be restarted manually after the successful installation of the COP file:

- Login to Cisco Unity Connection Serviceability Page and Navigate to Service Management, Stop and Start the Connection REST Tomcat service.
- Login to the administrator CLI of Cisco Unity Connection and use the command "utils service restart Cisco SSOSP tomcat" to restart the Cisco SSOSP Tomcat service
- If CUC is clustered, perform the above steps on both servers in the cluster.

If any issues are encountered, ciscocm.V14-SU2-SU2a_CSCwc26596_C0169-1_revert.k4.cop.sha512 (md5sum: d8dbd303c67bac3a23f6361a2a98d4a8) file can be used to revert the changes. If SSO is enabled, it will need to be disabled prior to performing the revert and re-enabled once the revert is complete.

Installation Instructions:

From Remote Source:

Step 1: Copy the COP file to an SFTP or FTP server.

Step 2: SSH to the admin CLI of the server

Step 3: Enter your OS Administrator username and password.

Step 4: Enter "utils system upgrade initiate"

Step 5: For the Source, choose SFTP

Step 6: Enter the Directory name for the cop file, if required.

If the cop file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the cop file is in the patches directory, you must enter /patches.

If the cop file is located on a Windows server, check with your system administrator for the correct directory path.

Step 7: Enter the required cop file information as described in the following table:

Server:	Host name or IP address of the remote server from which software will be downloaded.
User Name:	Name of a user who is configured on the remote server.
User Password:	Password that is configured for this user on the remote server.
Transfer Protocol:	Choose SFTP or FTP.
SMTP (optional):	Hostname of SMTP server for email alerts (if desired).

Step 8: Select Next to continue with the upgrade process.

Step 9: Choose the ***ciscocm.V14-SU2-SU2a_CSCwc26596_C0169-1.k4.cop.sha512*** COP file and select Next.

Step 10: In the next window, monitor the Download Status, which includes the filename and the number of megabytes that are getting transferred. When the download completes, the File Checksum Details window displays.

Step 11: Verify the checksum value:

Checksum for ***ciscocm.V14-SU2-SU2a_CSCwc26596_C0169-1.k4.cop.sha512***
md5sum: 6a099da8b63746a2f02bc2fc1e255cec

Step 12: After determining that the checksums match, click Next to proceed with the software upgrade.

Step 13: The Installation Status window is displayed. Monitor the Installation Status and the Installation Log. When the installation completes the Status will show Complete.

Step 14: Verify the COP file installed correctly using this command from the CLI:

admin:show version active
Active Master Version: <CUCM_Version>
Active Version Installed Software Options:
ciscocm.V14-SU2-SU2a_CSCwc26596_C0169-1.k4.cop.sha512